UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/281,852	03/31/1999	DARYL CARVIS CROMER	RP9-99-048	7708

45503 7590 11/18/2005		EXAMINER
DILLON & YUDELL LLP		TRUONG, THANHNGA B
8911 N. CAPITAL OF TEXAS HWY.,		

ART UNIT	PAPER NUMBER
2135	

SUITE 2110
AUSTIN, TX 78759

DATE MAILED: 11/18/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE BOARD OF PATENT APPEALS
AND INTERFERENCES

Application Number: 09/281,852
Filing Date: March 31, 1999
Appellant(s): CROMER ET AL.

Antony P. Ng
For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed August 19, 2004.

1.   ***Real Party in Interest***

A statement identifying the real party in interest is contained in the brief.

2.   ***Related Appeals and Interferences***

A statement identifying the related appeals and interferences which will directly

affect or be directly affected by or have a bearing on the decision in the pending appeal

is contained in the brief.

3.   ***Status of Claims***

The statement of the status of the claims contained in the brief is correct. This

appeal involves claims 1-7 and 10-16.

4.   ***Status of Amendements After Final***

No amendment after final has been filed.

5.   ***Summary of The Invention***

The summary of the invention contained in the brief is correct.

6.   ***Issues***

The appellant's statement of the issues in the brief is correct.

7.   ***Grouping of Claims***

The appellant's statement of the grouping of claims in the brief is correct.

8.   ***Claims Appealed***

The copy of the appealed claims contained in the Appendix to the brief is correct.

9.   ***Prior Art of Record***

| 6,182,142 | Win et al. | 1-2001 |
| 6,374,359 | Shrader et al | 04-2002 |

10.   Grounds of Rejection

The following grounds of rejection are applicable to the appealed claims:

Claims 1-7 and 10-16 are rejected under 35 U.S.C. 103(a) as being unpatentable over Win et al (US 6, 182,142), and further in view of Shrader et al (US 6, 374, 359 B1).

   a.   *Referring to claim 1:*

      i.   Win teaches:

         (1)   in response to the receipt of a cookie generated by an application from a remote server, encrypting said cookie with said public key **[i.e., if the name and password are correct, the Authentication Client Module reads the user's roles from the Registry Server 108. It then encrypts and sends this information in a "cookie" to the user's browser. A "cookie" is a packet of data sent by web servers to web browsers (column 6, lines 51-56). In addition, As shown by state 524, cookie 528 and cookie 530 are encrypted and returned to the browser 100. Alternatively, state 524 may involve digitally signing cookie 528 and cookie 530 using a digital signature algorithm. Preferably, the cookies are encrypted rather than digitally signed because encryption is faster and produces a smaller cookie (column 11, lines 1-8)]**;

         (2)   storing said encrypted cookie in a non-protected storage device within said data processing system **[i.e., referring to Figure 5C, cookie 528 and cookie 530 are saved in memory by the browser 100 indefinitely, unless either of the cookies expires, i.e., the system clock becomes equal to or greater than the expiration date value. The cookies 528, 530 are passed to each Web server that the user accesses and that is within the same domain as the Access Server 106. When a user quits the browser 100, cookies that have not expired are saved on a mass storage device associated with the browser 100, such as a disk drive located at the user's client machine or terminal (column 11, lines 11-18)]**;

(3)   in response to an access request for said encrypted cookie by a browser program executing within said data processing system, decrypting said encrypted cookie with said private key **[i.e., when the user selects a resource, the browser sends an open URL request and cookie to a Protected Web Server. A Protected Web Server is a web server with resources protected by the Runtime Module. The Runtime Module decrypts information in the cookie and uses it to verify that the user is authorized to access the resource (column 6, lines 65-67 through column 7, lines 1-3)]**; and

(4)   sending said decrypted cookie to said browser program **[i.e., the cookie is also used by the resource to return information that is customized based on the user's name and roles (column 7, lines 3-5)]**.

ii.   Although Win does not explicitly explain:

(1)   storing a encryption key pair having a private key and a public key in a protected storage device within said data processing system **[i.e., all transactions between components in the system are made using HTTP over SSL (Secure Sockets Layer) sessions. For example, browser 100 initiates an SSL session with a handshake during which it negotiates a hash function and session encryption key, that is "having a private key and a public key" with HTTP Server 402 of Access Server 106, that is "a protected storage device" for "storing a encryption key pair having a private key and a public key". Once the session is established, all data exchanged between browser 100 and HTTP server 402 is encrypted (column 22, lines 66-67 through column 23, lines 1-5)]**;

iii.   Shrader, on the other hand, teaches:

(1)   The key may comprise part of a public key cryptosystem (PKC - that is to employ an encryption key pair, such as a decryption private key and an encryption public key to decrypt and encrypt data), with the corresponding key being used for decryption in a known manner. A representative software PKC product is known in the art as PGP (Pretty Good Privacy), which is

available for download over the Internet. Other encryption techniques, such as a private key cryptosystem using a session key, or the like, may be used as well. Preferably, the key pair is constructed and stored locally (for root user access only) during configuration of the Web server **(column 7, lines 23-32)**.

      iv.   It would have been obvious to a person having ordinary skill in the art at the time the invention was made to:

      (1)   clearly disclose the storing of an encryption key pair for authenticating users of the access system 2 as in Figure 1 of Win.

      v.   The ordinary skilled person would have been motivated to:

      (1)   clearly disclose the storing of an encryption key pair for controlling access to protected information resources in a network environment, more specifically to methods, apparatus, and products for facilitating secure and selective access to network resources based on a role of a user of the resources **(column 1, lines 5-10 of Win).**

      b.   *Referring to claim 2:*

      i.   Win further teaches:

      (1)   wherein said non-protected storage device is a hard drive **[i.e., referring to Figure 9, a storage device 910, such as a magnetic disk, that is "a non-protected storage device", or optical disk (column 26, lines 17-18). In fact, a mass storage device associated with the browser 100, such as a disk drive, that is also "a non-protected storage device", located at the user's client machine or terminal (column 11, lines 16-18)]**.

      c.   *Referring to claim 3:*

      i.   Win further teaches:

      (1)   further comprising providing an encryption device having an encryption engine and said protected storage device accessible only through said encryption engine **[i.e., all transactions between components in the system are made using HTTP over SSL (Secure Sockets Layer) sessions. For example,**

browser 100 initiates an SSL session with a handshake during which it negotiates a hash function and session encryption key with HTTP Server 402 of Access Server 106.   Once the session is established, all data exchanged between browser 100 and HTTP server 402 is encrypted.   The SSL hash function is used to ensure data integrity, that is, to ensure that transactions are not tampered with or altered in any way. SSL encryption (that is "an encryption device having an encryption engine") is used to ensure that each transaction is private and confidential.   This means that no one can wiretap or eavesdrop and read the contents of transactions.   Thus no one can intercept names, passwords and cookies (column 22, lines 66-67 through column 23, lines 1-12)].

      d.   _Referring to claims 4, 5, 6, 7, 13, 14, 15, and 16:_

      i.   These claims have limitations that is similar to those of claim 3, thus they are rejected with the same rationale applied against claim 3 above.

      e.   _Referring to claim 10:_

      i.   This claim has limitations that is similar to those of claim 1, thus it is rejected with the same rationale applied against claim 1 above.

      f.   _Referring to claim 12:_

      i.   This claim has limitations that is similar to those of claim 3, thus it is rejected with the same rationale applied against claim 3 above.

11.   *Response to Arguments*

Regarding Appellant's arguments to Group I (claims 1-7 and 10-16) that the cited references do not teach or suggest a protected storage device for storing an encryption key pair and a non-protected storage device for storing encrypted cookies (see Appellant's Brief, page 5).

Examiner disagrees with the appellant because Win teaches in one embodiment, **all the components are stored on and executed by one physical server or computer**. And in alternate embodiments, one ore more components are installed on separate computers. For example, **Registry Server 108 may be part of a secure**

Intranet that is protected using a firewall 118, and Access Server 106 may be located on an extranet (that is remotely located) for access by users inside and outside the enterprise. Further, there may be more than one Registry Server 108 in a mirrored or replicated configuration. Each Access Server 106 may be coupled to more than one Registry Server 108, so that a particular Access Server 106 can communicate with a second Registry Server 108 if a first one is busy or unavailable. Each Registry Server 108 may be coupled to or support more than one Access Server 106 (column 4, lines 56-67 through column 5, lines 1-3). In addition, Win further teaches all transactions between components in the system are made using HTTP over SSL sessions. For example, browser 100 initiates an SSL session with a handshake during which it negotiates a hash function and **session encryption key** with HTTP Server 402 of Access Server 106. Once the session is established, **all data exchanged between browser 100 and HTTP server 402 is encrypted.** The SSL hash function is used to ensure data integrity, that is, to ensure that transactions are not tampered with or altered in any way. SSL encryption is used to ensure that each transaction is private and confidential. This means that no one can wiretap or eavesdrop and read the contents of transactions. **Thus no one can intercept names, passwords and cookies** (column 22, lines 65-67 through column 23, lines 1-12 of Win). Furthermore, Win also teaches a "cookie" is a packet of data sent by web servers to web browsers. Each cookie is saved by browser 100 until the cookie expires (column 6, lines 55-57 of Win). It is well-known in the art of computer network that browser is opened for general public used. Thus it is not restricted, not secure, and unsafe area. Therefore, everything that stores in this browser area will not be safe and protected. However, Win does not explicitly explain clearly how the encryption key pair being stored with the servers. On the other hand, Shrader teaches other encryption techniques, such as a private key cryptosystem using a session key, or the like, may be used as well. Preferably, **the key pair is constructed and stored locally (for root user access only)** during configuration of the Web server (column 7, lines 28-32 of Shrader). Thus, Win and Shrader, in combination, teach the claimed subject matter.

Appellant further argues that cited reference "Win" does not teach or suggest the cookie encryption being performed at the data processing system in which the browser resides, as claimed. A data processing system, by definition, is just a computer system which processes information after it has been encoded into data (see Wikipedia, the free encyclopedia). Furthermore, an assembly of computer hardware, firmware and software configured for the purpose of performing various operations on digital information elements with a minimum of human intervention (see Terminology Reference System). A server, by definition, (1) on a local area network (LAN) is also just another computer system for running administrative software that control access to the network and its resources, such as printer and disk drives, and provides resources to computers functioning as workstation on the network, (2) on the internet or other network, a computer or program that respond to command from a client. For example, a file server may contain an archive of data or program file; when a client submits a request for a file, the server transfers a copy of the file to client (see Microsoft Computer Dictionary, Fifth Edition). Therefore, data processing system and server have the same function and meaning. Win and Shrader, in combination, teach encryption key pair, which is public key and private key, whereby the Access Server of Win is for storing the encryption key. Thus, appellant's data processing system is just another entire system including a plurality of computer systems coupled with servers, etc. (see appellant's specification page 7 and appellant's drawing Figure 1) which is exactly demonstrated in Win's Figure 1 and the cookie encryption is executing and/or performing within the system where the browser is resided.

It is therefore shown that the components disclosed by Win and Shrader constitute the claimed a protected storage device for storing an encryption key pair and a non-protected storage device for storing encrypted cookies.

Regarding Appellant's arguments that the cited references do not teach or suggest **a hard drive for storing encrypted cookies** (see Appellant's Brief, page 6), it is noted that Appellant's arguments, **a hard drive for storing encrypted cookies,** do not even read into the claimed language at all as set forth in claim 2, "**wherein said non-protected storage device is a hard drive**" (see Appellant's Brief, page 6). In fact,
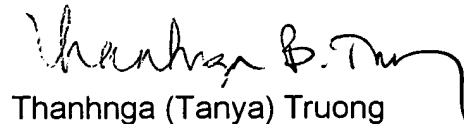
Win teaches when a user quits the browser 100, **cookies that have not expired are saved on a mass storage device associated with the browser 100, such as a disk drive (emphasis added)** located at the user's client machine or terminal. (column 11, lines 14-18 of Win). Therefore, it is believed that Win teaches the claimed   hard drive for storing encrypted cookies.

Regarding Appellant's arguments that Win does not teach or suggest an encryption device having an encryption engine (see Appellant's Brief, page 7), it is noted that all transactions between components in the system are made using HTTP over SSL (Secure Sockets Layer) sessions. For example, **browser 100 initiates an SSL session with a handshake during which it negotiates a hash function and session encryption key with HTTP Server 402 of Access Server 106.** Once the session is established, all data exchanged between browser 100 and HTTP server 402 is encrypted. The SSL hash function is used to ensure data integrity, that is, to ensure that transactions are not tampered with or altered in any way. **SSL encryption (that is "an encryption device having an encryption engine") is used to ensure that each transaction is private and confidential.** This means that no one can wiretap or eavesdrop and read the contents of transactions. Thus no one can intercept names, passwords and cookies (column 22, lines 66-67 through column 23, lines 1-12). Hence, Win teaches the claimed an encryption device having an encryption engine. Therefore, the combination of Win and Shrader is teaching the storing of encryption key pair.
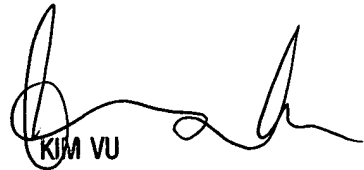
For the above reasons, it is believed that the rejections should be sustained.

Respectfully submitted,

Thanhnga (Tanya) Truong
October 31, 2005

KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

Conferees
Kim Vu
Hosuk Song

ANTONY P. NG
DILLON & YUDELL, LLP
8911 N. CAP. OF TEXAS HWY., SUITE 2110
AUSTIN, TEXAS 78759